

**Notice of Allowability**

Application No.

10/715,938

Examiner

Justin T. Darrow

Applicant(s)

WACK ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☐ This communication is responsive to \_\_\_\_.
2. ☒ The allowed claim(s) is/are 2-20.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some\* c) ☐ None of the:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.  
(a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached  
1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_.  
(b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |  |   |
|--|---|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)           |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 6. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date ____. |
| 3. <input checked="" type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),<br>Paper No./Mail Date <u>11/18/2003</u> | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment                   |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material                                 | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance  |
|  | 9. <input type="checkbox"/> Other ____.   |

### **DETAILED ACTION**

1. Claims 1-20 have been presented for examination. Claim 1 has been canceled and new claims 2-20 have been added in a preliminary amendment filed 11/18/2003. Claims 2-20 have been examined.

### **EXAMINER'S AMENDMENT**

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

The application has been amended as follows:

In the Specification:

Page 2 of Paper No. SPEC(11182003)(Amendments to the Written Description), line 2, after "09/418,806," insert --now U.S. Patent No. 6,684,330--.

### ***Priority***

3. Acknowledgment is made that the instant application is a continuation of Application No. 09/418,806, filed 10/15/1999, now U.S. Patent No. 6,684,330 B1, which claims benefit of the earlier filing date of provisional Application No. 60/104,512, filed 10/16/1998.

*Allowable Subject Matter*

4. Claims 2-20 are allowed.

5. The following is an examiner's statement of reasons for allowance:

Claims 2-11 are drawn to a method for providing a secure network packet. The closest prior art, Abadi et al., U.S. Patent No. 5,268,962 A. Abadi et al. discloses:

generating a working key (see column 3, lines 66-68; establishing a host-to-host key);

encrypting, based at least in part on the working key, target data (see column 3, lines 60-65; encrypting secure portions of data packets);

encrypting, based on at least in part on a cryptographic key, the working key (see column 4, lines 29-35; encrypting the Host-to-Host Key  $A_i$  with a Master Key); and

forming the secure network packet including the encrypted target data and the encrypted working key (see column 5, lines 7-21; figure 5A, step 211; encrypting a portion of the data packet and including the encrypted Host-to-Host Key  $A_i$ ),

wherein the plurality of key splits includes a domain key split and a user key split (see column 4, lines 64-68; figure 4, slot 146; Host-to-Host Key  $A_i$  is designated by the domain (see Microsoft Press Computer Dictionary, page 158; a subdivision in a network that can be formed by at least two computers) formed by the connection of Host A and Host I and the user (Host A)).

Although Abadi et al. describe generating the cryptographic key from a random number generator (see column 4, lines 15-19), this reference neither teaches nor suggests binding together a plurality of key splits to form a cryptographic key, wherein the plurality of key splits

Art Unit: 2132

includes a domain key split and a user key split. These distinct limitations explicitly recited in independent claim 2 render claims 2-11 allowable.

Claims 12-20 are drawn to a method of accessing encrypted target data encapsulated by a secure network packet. The closest prior art, Abadi et al., U.S. Patent No. 5,268,962 A. Abadi et al. discloses:

parsing the secure network packet to provide the encrypted target data and an encrypted working key (see column 5, lines 52-66; reading portions a received data packet); and

decrypting, based at least in part on a cryptographic key, the encrypted working key (see column 6, lines 29-31; decrypting the encrypted key with the Master Key);

decrypting, based at least in part on the decrypted working key, the encrypted target data to provide decrypted target data (see column 6, lines 57-60; decrypting the data packet).

However Abadi et al. neither shows nor motivates binding together a plurality of key splits to form the cryptographic key, wherein the plurality of key splits includes a domain key split and a user key split. These distinct limitations explicitly recited in independent claim 12 render claims 12-20 allowable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

### *Conclusion*

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Ganesan, U.S. Patent No. 5,737,419 A, discloses a cryptosystem involving key portions encrypted by authorized users in a network,
- Brands, U.S. Patent No. 5,696,827 A, describes cryptographic methods using user key portions.

### *Telephone Inquiry Contacts*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is 571-273-8300. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers

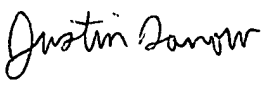
Application/Control Number: 10/715,938  
Art Unit: 2132

transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to 571-273-8300 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only **"OFFICIAL FAX"** but also **"AMENDMENT AFTER FINAL"**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

March 17, 2006

  
JUSTIN T. DARROW  
PRIMARY EXAMINER  
TECHNOLOGY CENTER 2100